PATENT CLAIMS

1. An information processing arrangement for converting message information from a first format into a second format, having a cipher unit (210) with a first cipher key input (212) and a data output (213) for outputting a data stream generated dependent on a first cipher key input via said first cipher key input (212), wherein said first cipher unit 210 includes: a memory (14) for storing data, means (16,11,12) for updating said memory with input information, an instruction table (13) comprising a set of operations adapted to modify said memory (14), processing means (11) adapted to select operations from said instruction table (13) in response to at least part of said input information, and to execute said selected operations on the contents of said memory (14), at least one of said set of operations being selectable in response to any possible configuration of at least part of said input information, and means (15) for extracting output information from said memory (14), **characterised in** that it is devised for encryption of information packets (220), each having a block head (221) and a plaintext data block (222) in a packet transmitting system.

2. An information processing apparatus according to claim 1, further being devised to separate the block head (221) from the plaintext data block (222) in connection with encryption; to encrypt the plaintext data block (222) and to assemble an encrypted information packet (230) including an unencrypted block head (231) and an encrypted data block (232) after said encryption.

3. An information processing apparatus according to claim 2, further being devised to, in connection with decryption, separate said unencrypted block head (231) and said encrypted data block (232) of said information packet (230), to decrypt the encrypted data block (232) and to assemble a decrypted information packet comprising a block head (221) and a plaintext data block (222).

4. An information processing apparatus according to claim 1, further comprising a look-up function (240) arranged to select a cipher key dependent on the content of the block head (221).

5. An information processing apparatus according to claim 4, wherein the look-

up function (240) is devised to select a cipher key for encryption and decryption, respectively, from a database (250).

6. An information processing apparatus according to claim 1, further being devised to change the destination address of the information block from a first to a second destination address in the output block head (231) dependent on the input block head (221).

7. An information processing apparatus according to claim 6, wherein the look-up function (240) is devised to select from a database (250) a data record (251) containing said second destination address.

8. An information processing apparatus according to claim 1, further comprising an assembly function (260) arranged in connection to the plaintext input to the cipher unit (210) for assembling a plurality of information packet (220) having the same destination address to a unified information packet with one block head and one plaintext block for encryption of said plaintext block to an encrypted data block.

9. An information processing apparatus according to claim 8, wherein the assembly function (260) further comprises compression means for the compression of the data block input to the cipher unit (210).

10. An information processing apparatus according to claim 8, further comprising an unpacking function (262) arranged in connection with a plaintext output of the cipher unit (210) for unpacking an assembled information packet (220) to separate information packets each having its block head and its plaintext block.

11. An information processing apparatus according to claim 9, wherein the unpacking function (260) further comprises the compression means for decompressing the data blocks output from the cipher unit (210).

12. An information processing apparatus according to claim 8, further being devised to assemble input information packets during a predetermined period of time.

13. An information processing apparatus according to claim 8, further comprising a resettable and presettable block arranged to be reset when a first

information packet is input to the assembly function (260), wherein the assembly of information packets continues until the clock reaches a preset value.

14. An information processing apparatus according to claim 10, further comprising a resettable and presettable clock devised to be preset when a first information packet is input to the unpacking function (262), wherein the unpacking of information packets continues until the clock reaches a preset value.

15. An information processing apparatus according to claim 1, which is adapted for encryption and decryption, respectively, of the information packets comprising any of:

multimedia information; a program part to an application program; a program part to a game program; a part of an image stream to HDTV; packets of the IP (Internet Protocol) type to the Internet; packets adapted to the ATM (Asynchronous Transfer Mode) [ITU I.321]; blocks according to the TCP (Transmission Control Protocol) level according to [RFC 793]; blocks according to the UDP (User Datagram Protocol) according to [RFC 793]; blocks according to the IPSEC [RFC 2406]; blocks according to the SMTP [RFC 821]; blocks according to the Secure Sockets Layer [RFC SSL]; blocks according to the WAP (Wireless Application Protocol); blocks in the Transaction layer, WTP (Wireless Transaction Protocol); blocks in the Security layer, WTLS – Wireless Transport Layer Security; or blocks according to the WDP (Wireless Datagram Protocol).

16. A computer implemented information processing method for converting message information from a first format to a second format, comprising a first encryption algorithm (930), wherein said first encryption algorithm comprises the steps of:

establishing a set of operations for modifying the state of a memory,

storing input information in a first format in said memory,

selecting operations from said set in response to at least part of said input information and executing said operations on information stored in said memory, wherein said set of operations is devised such that an operation can be selected in response to any possible input information stream, and

extracting information from said memory in a second format after executing

at least one operation, **characterised in** a step of encrypting information packets (220), comprising a block head (221) and a plaintext data block (222), in a packet transmitting system.

17. An information processing method according to claim 16, further comprising the steps of separating the block head (221) from the plaintext data block (222) in connection with encryption; encrypting the plaintext data block (222) and after said encryption assemble an encrypted information packet (230) comprising an unencrypted block head (231) and an encrypted data block (232).

18. An information processing method according to claim 16, further comprising the steps of separating said unencrypted block head (231) and encrypted data block (232) of said information packet (230) in connection with decryption, decrypting the encrypted data block (232) and assembling a decrypted information packet comprising a block head (221) and a plaintext data block (222).

19. An information processing method according to claim 16, further comprising the step of selecting a cipher key dependent on the block head (221).

20. An information processing method according to claim 16, further comprising the step of selecting from a database (250) a cipher key for encryption and decryption, respectively.

21. An information processing method according to claim 16, further comprising the step of changing the destination address of the information block from the first to the second destination address in the output block head (231) dependent on the input block head (221).

22. An information processing method according to claim 16, further comprising the step of selecting from a database (250) data record (251) containing said destination address.

23. An information processing method according to claim 16, further comprising the step of assembling in connection with inputting the plaintext to the cipher algorithm (210) a plurality of information packets (220) with the same destination address to an assembled information packet having one block head and one plaintext block and encrypting said plaintext block to an encrypted data block.

24. An information processing method according to claim 16, further comprising

the step of compressing the data blocks input to the cipher unit (210).

25. An information processing method according to claim 16, further comprising the step of unpacking in connection with outputting the plaintext from the cipher algorithm and assembled information packet (220) to separate information packets each having its block head and its plaintext block.

26. An information processing method according to claim 16, further comprising the step of decompressing the data blocks output from the cipher unit (210).

27. An information processing method according to claim 23, further comprising the step of assembling input information packets for a predetermined period of time.

28. An information processing method according to claim 23, further comprising the step resetting a preset clock when the first information packet is input to the assembling step (260) wherein the assembling of information packets continues until the clock reaches a preset value.

29. An information processing method according to claim 25, further comprising the step of resetting a preset clock when a first information packet is input to the unpacking step (262), wherein the unpacking of information packets continues until the clock reaches a preset value.

30. An information processing apparatus according to claim 16, which is adapted for encryption and decryption, respectively, of the information packets comprising any of:

multimedia information; a program part to an application program; a program part to a game program; a part of an image stream to HDTV; packets of the IP (Internet Protocol) type to the Internet; packets adapted to the ATM (Asynchronous Transfer Mode) [ITU I.321]; blocks according to the TCP (Transmission Control Protocol) level according to [RFC 793]; blocks according to the UDP (User Datagram Protocol) according to [RFC 793]; blocks according to the IPSEC [RFC 2406]; blocks according to the SMTP [RFC 821]; blocks according to the Secure Sockets Layer [RFC SSL]; blocks according to the WAP (Wireless Application Protocol); blocks in the Transaction layer, WTP (Wireless Transaction Protocol); blocks in the Security layer, WTLS – Wireless Transport Layer Security; or blocks according to the WDP (Wireless Datagram Protocol).

31. A computer program product for use in a data processing system for converting message information from a first format to a second format, comprising means for directing the data processing system to perform a first cipher algorithm (930), wherein said first cipher algorithm comprises the steps of:

establishing a set of operations for modifying the state of a memory,

storing input information in a first format in said memory,

selecting operations from said set in response to at least part of said input information and executing said operations on information stored in said memory, wherein said set of operations is devised such that an operation can be selected in response to any possible input information stream, and

extracting information from said memory in a second format after executing at least one operation, **characterised in**

means for directing the data processing system to encrypt information packets (220), comprising a block head (221) and a plaintext data block (222), in a packet transmitting system.

32. A computer program product according to claim 31, further comprising means for directing the data processing system to, in connection with encryption, separate block head (221) from the plaintext data block (222); to encrypt the plaintext data block (222) and to, after said encryption, assemble an encryption information packet (220) having an unencrypted block head (231) and an encrypted data block (232).

33. A computer program product according to claim 31, further comprising means for directing the data processing system to, in connection with decryption, separate said unencrypted block head (231) and encrypted data block (232) of said information packet (230), to decrypt the encrypted data block (232) and to assemble a decrypted information packet having a block head (221) and a plaintext data block (222).

34. A computer program product according to claim 31, further comprising means for directing the data processing system to select a cipher key dependent on the content of the block head (221).

35. A computer program product according to claim 31, further comprising

means for directing the data processing system to select from a database (250) a cipher key for encryption and decryption, respectively.

36. A computer program product according to claim 31, further comprising means for directing the data processing system to change the destination address of the information block from a first to a second destination address in the output block head (231) dependent on the input block head (221).

37. A computer program product according to claim 31, further comprising means for directing the data processing system to select from a database (250) a data record (251) containing said second destination address.

38. A computer program product according to claim 31, further comprising means for directing the data processing system to assemble, in connection with the input of plaintext to the cipher algorithm (210), a plurality of information packets (220) with the same destination address to an assembled information packet with one block head and one plaintext block and to encrypt said plaintext block to an encrypted data block.

39. A computer program product according to claim 31, further comprising means for directing the data processing system to compress the data blocks input to the cipher algorithm (210).

40. A computer program product according to claim 31, further comprising means for directing the data processing system to unpack, in connection with the output of plaintext from the cipher algorithm, an assembled information packet (220) to separate information packets each having its block head and its plaintext block.

41. A computer program product according to claim 31, further comprising means for directing the data processing system to decompress the data blocks output from the cipher algorithm (210).

42. A computer program product according to claim 38, further comprising means for directing the data processing system to assemble input information packets during a predetermined period of time.

43. A computer program product according to claim 38, further comprising means for directing the data processing system to reset a preset clock were a first

information packet is input to the assembled step (260), wherein the assembly of information packets continues until the clock reaches a preset value.

44. A computer program product according to claim 40, further comprising means for directing the data processing system to reset a preset clock when a first information packet is input to the unpacking step (262), wherein the unpacking of information packets continues until the clock reaches a preset value.

45. A computer program product according to claim 31, further comprising means for directing the data processing system to encrypt and decrypt, respectively, information packets containing any of:

multimedia information; a program part to an application program; a program part to a game program; a part of an image stream to HDTV; packets of the IP (Internet Protocol) type to the Internet; packets adapted to the ATM (Asynchronous Transfer Mode) [ITU I.321]; blocks according to the TCP (Transmission Control Protocol) level according to [RFC 793]; blocks according to the UDP (User Datagram Protocol) according to [RFC 793]; blocks according to the IPSEC [RFC 2406]; blocks according to the SMTP [RFC 821]; blocks according to the Secure Sockets Layer [RFC SSL]; blocks according to the WAP (Wireless Application Protocol); blocks in the Transaction layer, WTP (Wireless Transaction Protocol); blocks in the Security layer, WTLS – Wireless Transport Layer Security; or blocks according to the WDP (Wireless Datagram Protocol).